UNITED STATES DISTRICT COURT

for the

District of Maryland

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Subject Electronic Devices Described in Attachment A

Case No. 15 - 172 BPG

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the District of MARYLAND, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. Section 841(a)(1)	Distribution and Possession with the Intent to Distribute Narcotics

The application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TFO Paul Geare, ATF
Printed name and title

Sworn to before me and signed in my presence.

Date: 1-29-15

Judge's signature

City and state: Baltimore, MD

Beth P. Gesner, United States Magistrate Judge
Printed name and title

ATTACHMENT A – DESCRIPTION OF LOCATIONS TO BE SEARCHED

The devices to be searched are (1) Kyocera Model C5170, FCC ID: V65C5170, DEC: 268 435 459 911 209 019; (2) Samsung Model SGH-T599N, FCC ID: A3LSGHT599, Serial# 356433/05/068789/9; (3) Gray Samsung flip phone Model SCH-U365, SKU: SCHU365HPP, FCC ID: A3LSCHU365, MEID HEX: A000004078F92E; (4) Cricket LG Model LW690, FCC ID: BEJMS690, Serial# 104KPAE0131568, MEID: 268435460015869350; (5) Samsung Model SPH-M830, FCC ID: A3LSPHM830, DEC: 268 435 461 708 029 164, HEX: A00 000397 A83 EC; (6) Blackberry 8330 IC: 2503A-RBU20CW, FCC ID: L6ARBU20CW, ESN HEX: 4C343AA9; and (7) Samsung Boostmobile Model SPH-M580, FCC ID: A3LSPHM580, DEC: 268435460804146914, HEX: A00000303F46E2. The devices are in custody with the Bureau of Alcohol, Tobacco, Firearms and Explosives, Baltimore. The devices will be charged and powered on. The devices and all readable and searchable contents will be downloaded and then be copied to a readable computer disc and reviewed by your affiant. A search warrant return will be provided to the Court thereafter.

ATTACHMENT B – SEARCH PROTOCOLS

The **SUBJECT ELECTRONIC DEVICE(S)** more fully identified in Attachments A may be searched for the following items, which may be seized:

All records, documents, items, data and other information that may constitute fruits or instrumentalities of, or contain evidence related to violations of 21 U.S.C. §§ 841(a)(1) and 846, including, but not limited to, the following:

1. Information that identifies unknown co-conspirators and accomplices;

2. The location of stash houses for money and/or narcotics;

3. Information pertaining to narcotics trafficking, including but not limited to quantities sold, pricing, monies owed, accounts receivable, purchaser information, and correspondence (including e-mail, text messages, and other electronic correspondence);

4. Mobile phone numbers and addresses utilized by co-conspirators and accomplices in this criminal conspiracy;

5. Any and all documents that identify and depict a relationship with conspirators, including: (a) photographs; (b) phone bills and call logs; (c) phone books; (d) address books; and (e) text messages, email, and electronic correspondence.

Because of the possibility that the files examined pursuant to the warrant will include information that is beyond the scope of what the United States has demonstrated the existence probable cause to search for, the search shall be conducted in a manner that will minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search is not viewed.

Because of the possibility that the files examined pursuant to the warrant will include information that is beyond the scope of what the United States has demonstrated the existence probable cause to search for, the search shall be conducted in a manner that will minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search is not viewed.

While this protocol does not prescribe the specific search protocol to be used, it does contain limitations to what government investigators may view during their search, and the searching investigators shall be obligated to document the search methodology used in the event that there is a subsequent challenge to the search that was conducted, pursuant to the following protocol:

With respect to the search of any digitally/electronically stored information that is seized pursuant to this warrant, and described in Attachment A hereto, the search procedure shall include such reasonably available techniques designed to minimize the chance that the government investigators conducting the search will view information that is beyond the scope for which probable cause exists.

The following list of techniques is a non-exclusive list which illustrates the types of search methodology that may avoid an overbroad search, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein:

a. Use of computer search methodology to conduct an examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth herein by specific date ranges, names of individuals, or organizations;

b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;

c. Physical examination of the storage device, including digitally surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth herein; and

d. Opening or reading portions of files that are identified as a result of conducting digital search inquiries in order to determine their relevance.